have a reduced level of emanations (e.g., approved by the Subcommittee on Compromising Emanations) or located in an area with a sufficient perimeter of control.

(d) Typewriter ribbons used in typing classified information shall be protected in the same manner as the highest level of classification for which they have been so used. When destruction is necessary, it shall be accomplished in the manner prescribed for classified working papers (See subpart H) of the same classification. After the upper and lower sections of the ribbon have been cycled through the typewriter five times in the course of regular typing, all fabric ribbons may be treated as unclassified. Carbon and plastic typewriter ribbons and carbon paper which have been used in the production of classified information shall be destroyed after initial usage in the manner prescribed for working papers of the same classification. As an exception to the foregoing, any typewriter ribbon which remains substantially stationary in the typewriter after it has received at least five consecutive impressions may be treated as unclassified.

§ 17.81 Care after working hours.

Heads of Offices, Boards, Divisions and Bureaus shall require and institute through their Security Programs Managers, a system of security checks at the close of each working day to ensure that the classified information in the possession of such Offices, Boards, Divisions and Bureaus is properly protected. Security Programs Managers shall require the custodians of classified information in their Offices, Boards, Divisions or Bureaus to make periodic inspections of their respective areas which shall ensure that the following minimum requirements are met:

(a) All classified information is stored in approved security containers. This includes removable storage media, e.g., floppy disks used by word processors, that contain classified information.

(b) Burn bags, if utilized, are either stored in approved security containers or destroyed.

(c) Classified shorthand notes, carbon paper, carbon and plastic typewriter ribbons, rough drafts and similar papers have been properly stored or destroyed.

§ 17.82 Administrative aids for safeguarding classified material.

Appropriate forms shall be used on security containers for check purposes. Such forms shall be conspicuously attached to the outside of each container used for the storage of classified information. Each authorized person will record the time and date that he or she unlocks or locks the security container, followed by the person's initials. At the close of each working day, a person other than the individual locking the container will check the container, in the presence of the individual locking the container, to ensure that it is secure. The time of the check followed by the checker's initials will be recorded. The check will be conducted each working day. If a container has not been opened, the date and the phrase ''Not Opened'' will be noted in addition to the time and the checker's initials. A container will not be left unattended until it has been locked by an authorized person and checked by a second person. The person locking a container is responsible for insuring that another person checks the container. Reversible ''OPEN-CLOSED'' signs, shall be utilized on security containers containing classified information. The respective side of the sign shall be displayed to indicate when the container is open or closed.

§ 17.83 Telephone or telecommunication conversations.

(a) Classified information shall not be discussed over nonsecure telephones. Classified telephone conversations are authorized only over approved secure (encrypted) communication circuits. Information concerning which telephones in the Department are secure may be obtained from Security Programs Managers or the Department Security Officer.

(b) Classified information shall not be transmitted over nonsecure radio equipment or facsimile devices. Classified information may be transmitted

using approved secure (encrypted) communication equipment. Guidance on which communication equipment is secure may be obtained from the Security Programs Manager or the Department Security Officer.

§17.84 Security of meetings and conferences.

The official responsible for arranging or convening a conference or other meeting is also responsible for instituting procedures and selecting facilities which provide adequate security if classified information is to be discussed or disclosed. (See Department Order 2660.1A.) The responsible official will:

(a) Notify each person who is to be present or who is to discuss classified information or any security limitations that must be imposed because of:

(1) The level of access authorization.

(2) Requirement for access to the information by the attendees.

(3) Physical security conditions.

(b) Ensure that each person attending the classified portions of meetings has been authorized access to information of equal or higher classifiation than the information to be disclosed.

(c) Ensure that the area in which classified information is to be discussed affords adequate acoustical security against unauthorized disclosure.

(d) Ensure that adequate storage facilities are available, if needed.

(e) Control and safeguard any classified information furnished to those in attendance and retrieve the material or obtain receipts, as required.

(f) Monitor the meetings to ensure that discussions are limited to the level authorized.

(g) Ensure that meetings at which classified information is to be discussed will be held only in a U.S. Government area or at a cleared facility of a Department contractor or consultant. When necessary for the accomplishment of essential functions, a meeting involving classified information may be held at another location provided it has been specifically authorized by the Department Security Officer.

Subpart F—Foreign Government Information

§17.85 Identification of documents.

Foreign Government Information under this regulation is of two types and shall be classified in accordance with this subpart.

(a) Information, whether classified or unclassified, provided by a foreign government or governments, an international organization of governments, or any element thereof with the expectation, express or implied, that the information, the source of the information, or both, are to be held in confidence shall be classified by the Office, Board, Division, or Bureau receiving the document.

(b) Information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence shall be classified.

§17.86 Classification.

(a) Foreign Government Information classified and provided by a foreign government or international organization of governments shall retain its original classification designation or be assigned a United States classification designation that will ensure a degree of protection equivalent to that required by the government or organization that furnished the information. Original classification authority is not required for this purpose.

(b) Foreign Government Information that was not classified by a foreign entity but was provided with the expectation, expressed or implied, that it be held in confidence must be classified. Therefore, such Foreign Government Information shall be classified at least Confidential, and higher whenever the damage criteria for Secret and Top Secret in subpart B are determined to be met.

§17.87 Presumption of damage by unauthorized disclosure.

Unauthorized disclosure of Foreign Government Information, the identity